PREFACE TO SELECTED INFORMATION DIRECTIVES

CIO Transmittal No.: 15-010	CIO Approval Date: 06/12/2015

Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19, dated 07/07/2005

CHIEF INFORMATION OFFICER MEMORANDUM

SUBJECT: Chief Technology Officer (CTO) Responsibilities in Selected Information Directives

Re-assigned CTO responsibilities

Effective immediately, CTO responsibilities detailed in the selected information directives (i.e., Information Policies, Procedures, Standards, and Guidance) listed in Appendix A are re-assigned to the OEI Office of Technology, Operations, and Planning (OTOP) Director and the Senior Agency Information Security Officer (SAISO) as detailed. The re-assignment does not change any requirements in the selected information directives.

The OEI Information Directives Program Manager is directed to attach this memorandum and Appendix A as a Preface to each of the Information Directives listed. OEI will then update the Roles and Responsibilities section of each Information Directive in accordance with the normal review and update cycle.

Ann Dunkin
Chief Information Officer
U.S. Environmental Protection Agency

APPENDIX A

Information Directive	Prior CTO Responsibilities	Re-assignment
CIO 2104.1 Software Management and Piracy Policy	Provide procedures, standards, and guidance to senior level managers to: support the Agency's Software Management and Piracy Policy and manage enterprise software licenses.	OTOP Director
CIO 2104-P-01.0 Software Management and Piracy Procedure	Provide procedures, standards, and guidance to senior level managers to: support the Agency's Software Management and Piracy Policy, manage enterprise software licenses, and provide covered users within their office with training and awareness on the Software Management and Piracy Policy through the annual Cybersecurity Awareness Training.	OTOP Director
CIO 2121.1 System Life Cycle Management (SLCM) Policy	Establish and publish procedures, technical operational procedures and standards (TOPS), and guidance supporting the Agency's SLCM Policy. Review and approve waivers to the SLCM Procedure.	OTOP Director
CIO 2121-P-03.0 SLCM Procedure	Establish and publish procedures, TOPS, and guidance supporting the Agency's SLCM Policy. Review and approve waivers to the SLCM Procedure.	OTOP Director
CIO 2122.1 Enterprise Architecture (EA) Policy	Issue procedures, guidance, and technical standards associated with the EA with a specific focus on the technology architecture, chair the Quality Technology Subcommittee (QTS), and review technology and security considerations in the Enterprise Target Architecture and Enterprise Transition Plan.	OTOP Director
CIO 2122-P-01.1 EA Governance Procedures	Issue procedures, guidance, and technical standards associated with the EA, with a specific focus on the technology architecture, chair the QTS, and review technology and security considerations in the Enterprise Target Architecture and Enterprise Transition Plan.	OTOP Director
CIO 2122-P-03.0 Information Technology Infrastructure Standard Procedure	Recommend to the CIO a specific IT standard, product or specification to be added to the official Agency IT Standards Profile with consultation from the Quality Information Council (QIC) and the QTS, and develop and maintain the Agency's Technology Architecture.	OTOP Director
CIO 2122-S-02.0 Personal Computer Configuration and Management Standard	Review and approve requests for waivers in regard to this standard.	OTOP Director
CIO 2123.1 Configuration Management Policy	Provide procedures, standards, and guidance to senior level managers in support of the Agency's Configuration Management Policy; institute change management processes; and provide a change management database.	OTOP Director

Information Directive	Prior CTO Responsibilities	Re-assignment
CIO 2150-P-01.1 Information Security - Interim Access Control Procedures	Approve all methods of dial-up access, approve all wireless connections, establish, document, authorize, and monitor all methods of remote access to an information system; delegate to Regions and other entities, as appropriate; and address co-management responsibilities for the Agency Security Architecture.	OTOP Director
CIO 2150-P-08.1 Information Security - Interim Incident Response Procedures	Determine Operational Status Categories during Alerts and Risks (OSCAR) 5 level (page 7).	SAISO
	Be available when the Computer Security Incident Response Capability (CSIRC) must report and coordinate incidents (page 16). Be available to meet with the Director of Cyber Security Staff (CSS) when senior managers are informed of incidents, occurrences and their status (page 18).	OTOP Director
CIO 2150-P-14.1 Information Security - Interim Risk Assessment Procedures	Approve the use of and, as appropriate, acquire and deploy enterprise vulnerability management technology. Consult with the SAISO to determine the coverage and compliance of enterprise vulnerability management technology with respect to federal and Agency requirements, including use of these tools to meet assessment requirements of other control families in NIST 800-53A, Revision 1, and to ensure the most cost effective, complete and accurate results.	OTOP Director
CIO 2150-P-15.1 Information Security - Interim System Services Acquisition Procedures	For the procurement of external information system services where a sufficient level of trust cannot be established, be available to confer regarding risks associated with the network and the Agency.	OTOP Director
CIO 2150-P-16.1 Information Security - Interim System and Communications Protection Procedures	Approve use of mobile VoIP-enabled units.	OTOP Director
CIO 2150.4 Mobile Computing Policy	Oversee policy and procedure implementation regarding use of mobile computing technologies. Approve mobile computing technology and device deployment.	OTOP Director
CIO 2150-P-01.1 Mobile Computing Management Procedures	Oversee policy and the implementation of the procedures. Approve enterprise mobile device types to be deployed. Review and approve requests for waivers in regards to the procedures.	OTOP Director

EPA INFORMATION PROCEDURES

OFFICE OF ENVIRONMENTAL INFORMATION

EPA Classification No.:	CIO-2150.3-P-15.1	CIO Approval Date:	08/06/2012
CIO Transmittal No.:	12-003	Review Date:	08/06/2015

Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19, dated 07/07/2005

INFORMATION SECURITY –
INTERIM SYSTEM AND SERVICES ACQUISITION PROCEDURES
V3.1
JULY 17, 2012

1. PURPOSE

The purpose of this procedure is to facilitate the implementation of Environmental Protection Agency (EPA) security control requirements for the System and Services Acquisition control family, as identified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 3 *Recommended Security Controls for Federal Information Systems and Organizations*.

2. SCOPE AND APPLICABILITY

These procedures cover all EPA information and information systems to include those used, managed, or operated by a contractor, another agency, or other organization on behalf of the Agency.

These procedures apply to all EPA employees, contractors, and all other users of EPA information and information systems that support the operation and assets of EPA.

3. AUDIENCE

These procedures apply to all EPA employees, contractors, and all other users of EPA information and information systems that support the operations and assets of EPA.

4. BACKGROUND

Based on federal requirements and mandates, the EPA is responsible for ensuring that all Offices within the Agency meet the minimum security requirements defined in the Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*. All EPA information systems must meet the security requirements through the use of the security controls defined in the NIST SP 800-53, Revision 3 *Recommended Security Controls for Federal Information Systems and Organizations*. This chapter addresses the procedures and standards set forth by EPA, and in compliance with, the system and services acquisition family of controls found in NIST SP 800-53, Revision 3.

EPA Classification No.:	CIO-2150.3-P-15.1	CIO Approval Date:	08/06/2012
CIO Transmittal No.:	12-003	Review Date:	08/06/2015

5. AUTHORITY

- E-Government Act of 2002, Public Law 107-347, Title III*, Federal Information Security Management Act (FISMA)* as amended
- Freedom of Information Act (FOIA), 5 U.S.C. § 552, as amended by Public Law 104-231, 110 Stat. 3048, Electronic Freedom of Information Act Amendments of 1996
- Clinger-Cohen Act of 1996, Public Law 104-106
- Paperwork Reduction Act of 1995 (44 USC 3501-3519)
- Privacy Act of 1974 (5 USC § 552a) as amended
- USA PATRIOT Act of 2001, Public Law 107-56
- Code of Federal Regulations, Part 5 Administrative Personnel, Subpart C—*Employees Responsible for the Management or Use of Federal Computer Systems*, Section 930.301 through 930.305 (5 C.F.R 930.301-305)
- Federal Acquisition Regulation (FAR) Part 39—*Acquisition of Information Technology*
- Office of Management and Budget (OMB) M-00-07, "Incorporating and Funding Security in Information Systems Investments", February 2000
- OMB Memorandum M-07-18, "Ensuring New Acquisitions Include Common Security Configurations", June 2007
- OMB Memorandum M-09-25, "Improving Government Acquisition", July 2009
- OMB Memorandum M-09-26, "Managing the Multi-Sector Workforce", July 2009
- OMB Memorandum M-10-27, "Information Technology Investment Baseline Management Policy", June 2010
- OMB Circular A-11, "Preparation, Submission, and Execution of the Budget", July 2010
- OMB Circular A-130, "Management of Federal Information Resources", Appendix III, "Security of Federal Information Automated Resources", November 2000
- Federal Information Processing Standards (FIPS) 140-2, *Security Requirements for Cryptographic Modules*, May 2001
- FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004
- FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006
- EPA Information Security Program Plan
- EPA Information Security Policy

6. PROCEDURES

SA- 2 – Allocation of Resources

a. The resources required to provide security for the information system must be determined, documented, and allocated as part of the capital planning and

investment control process.

b. Security must be integrated into the Capital Planning and Investment Control (CPIC) process as follows:
    i. Comply with the Agency's capital asset budget planning process.
    ii. Follow a methodology consistent with NIST SP 800-65, OMB Circular A-11, and related memoranda and guidance.

c. Information security requirements for the information system must be included in mission/business process planning.
    i. IT security priorities and requirements at the project and enterprise level must be integrated into business cases and the related OMB Exhibit 53 and Exhibit 300 documentation.
    ii. Business case analysis must consider how to employ and leverage existing federal and Agency components of the security architecture and standards, including common controls, before new technology control investments may be proposed.
    iii. Exhibit 53 and Exhibit 300 must be reviewed annually for IT security consistency and compliance with all related information including, but not limited to, information in the EPA repository (e.g., dates, system criticality details including Business Area, Line of Business, Information Type, Privacy Act).

d. Linkage must be maintained between more detailed operational budget plans and OMB Exhibit 53 and 300 to ensure accountability of resources.

e. For information system assets that are considered critical (e.g., mission critical, continuity of operations or government, critical infrastructure), EPA shall ensure the criticality designations are consistent with other reporting data (e.g., FIPS 199 system categorization, system criticality details, OMB submissions) and reflected in the Business Impact Assessments (BIA), as applicable.
    i. Refer to *Information Security – Interim Contingency Planning Procedures* for requirements on BIA.

f. Annual security requirements and associated tasks and resources must be addressed as listed in OMB Exhibit 53 instructions within the business cases and accounted for over the investment life cycle.
    i. The security requirements and associated tasks include but are not limited to:
        - Risk Assessment.
        - System Security Plan (SSP).
        - Security Authorization.
        - Reporting.
        - Plan of Action and Milestones (POA&M) tasks and milestones.
        - Background screening.
        - Annual Contingency Plan testing.
        - Annual control assessments and continuous monitoring.

- Architectural sequence planning.
- Computer security awareness and training:
  - Annual security awareness and training / refresher training.
  - Specialized security training / refresher training.

ii. It is expected that security costs will increase throughout the Development Phase of the life cycle and then enter a relative steady state during the Operations and Maintenance (O&M) Phase.

- During O&M, variations of resource requirements may occur due to periodic activities (e.g., security authorization) or unexpected requirements (e.g., court decisions, changes in governing statutes).
- Good planning practices and continuous monitoring must be used to prevent or reduce the likelihood of unexpected resource requirements.

iii. Security requirements and resource requirements associated with significant changes for the information system must be planned and budgeted.

- Percentage budget figures for current year and budget year for IT security must be based on a roll-up of these resource needs.

g. A discrete line item for information security must be established in organizational programming and budgeting documentation.

h. For systems in development, the following security requirements must be line items in the project work breakdown structure with its associated resource requirements and dates:

i. FIPS 199 security categorization.
ii. Risk Assessment.
iii. Privacy Impact Assessment (PIA).
iv. SSP.
v. POA&M tasks and milestones.
vi. Contingency Plan training and testing.
vii. Interconnection Security Agreements, Memoranda of Understanding/Agreement (MOU/A), and Service Level Agreements (SLAs), if applicable.
viii. Security controls assessment.
ix. Security Authorization.
x. Computer security awareness and training.
xi. Implementation.

i. For systems in operations and maintenance, the following security requirements must be line items in the project work breakdown structure with its associated resource requirements and dates:

i. FIPS 199 security categorization review.
ii. PIA, as applicable to changes and privacy requirements.
iii. Risk Assessment update or revision.

iv. SSP update or revision.
v. POA&M tasks and milestones.
vi. Contingency Plan training, testing and revision.
vii. Security controls assessment.
- Associated with planned configuration changes or modifications.
- Associated with annual requirements for assessment.

viii. Continuous monitoring.
ix. Interconnection Security Agreement and MOU/MOA review and revision, if applicable.
x. Disposition Plan, if applicable.
xi. Computer security awareness and training.
xii. Configuration management activities and related modifications.

j. The EPA designated repository must be used and maintained as EPA's authoritative source for relevant CPIC reporting and budgetary planning.
i. CPIC data and data in the EPA repository must be consistent.
ii. The EPA repository must be used to enter and maintain dates for key information system security milestones and requirements, including but not limited to the following:
- Risk Assessment dates.
- Authorization to operate date.
- Approved SSP date.
- POA&M milestone dates.

iii. The EPA repository must be used to maintain other key information system security data such as FIPS 199 security categorization.
- Refer to *Information Security – Interim Security Planning Procedures* for requirements on security categorization.

SA- 3 – Life Cycle Support

a. The information system must be managed using a system development life cycle (SDLC) methodology that includes information security considerations.
i. NIST SP 800-64, Revision 2 must be used as guidance on security considerations in the SDLC.

b. Information system security roles and responsibilities must be defined and documented throughout the SDLC.
i. Individuals having information security roles and responsibilities must be identified.

c. Once EPA has completed the next review and update of CIO 2121-P-01.0, System Life Cycle Management Procedure, EPA shall adhere to NIST SP 800-64, Revision 2 as a required guideline for integrating security considerations in the SDLC.
i. Control gates, or established points in the life cycle, must be used to determine whether the project should continue as is, change direction, or be

discontinued.

ii. Key outputs, in the form of deliverables or artifacts, for common tasks must be generated.

- Expected outputs must provide information vital to the system design.

Note: The updated System Life Cycle Management Procedure and NIST SP 800-64, Revision 2 will involve certain re-alignments of life cycle phases for EPA:

i. The Initiation Phase maps roughly to EPA's Definition Phase.

- *Security Planning begins in this phase and includes the following initial activities:*
  - *Categorization of information and the information system.*
  - *Security risk assessment.*
  - *Selection of baseline controls, which are then to be included as requirements for the Acquisition and Development Phase.*
  - *Privacy threshold and impact assessments.*

ii. The Acquisition and Development Phase maps appropriately, although with differences in details.

- *Activities that NIST identifies as beginning in this phase are, under EPA procedures, identified as being started in the Initiation/Definition Phase and thus updated in this phase.*

iii. The Operations and Maintenance Phase encompasses EPA's Implementation, and Operations and Maintenance Phases.

iv. The Disposal Phase maps to EPA's Termination (Retirement) Phase.

SA- 4 – Acquisitions

a. Requirements and/or specifications must include the following, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.
   i. Security functional requirements/specifications
   ii. Security-related documentation requirements
   iii. Developmental and evaluation-related assurances requirements

b. Acquisition packages must be reviewed for compliance with all requirements in this procedure.

c. Acquisition documents (e.g., requests for proposals) for information systems, information system components, and information system services must include, either explicitly or by reference, security requirements and/or specifications that describe:
   i. Required security capabilities (i.e., security needs and, as necessary, specific security controls and other specific FISMA requirements).
   ii. Required design and development processes.

iii. Required test and evaluation procedures.

iv. Required documentation.

- The level of detail required in the documentation must be based on the security categorization for the information system.
- Documentation must address user and system administrator guidance and information regarding the implementation of the security controls in the information system.
- Documentation must include security configuration settings and related security implementation guidance.

v. Security controls must be updated under circumstances including, but not limited to, the following:

- As new threats/vulnerabilities are identified.
- As new technologies are implemented.

vi. Contractors' security responsibilities.

vii. Contractors' level of screening or security supervision required.

- Refer to *Information Security – Interim Personnel Security Procedures* for requirements on screening.

viii. Conformance to mandates of the United States Government Configuration Baseline (USGCB) for any system-level software that is to be installed and run on an Agency desktop or laptop must be adhered to.

- The software must adhere to USGCB configuration settings.
- Software updates must not alter USGCB configuration settings.
- Justifications for exemptions or deviations must be documented in writing.

d. The procurement of non-standard, system-level software that is to be installed on any EPA information system must be approved.

e. OMB must be used as guidance on configuration management and acquisition requirements.

i. Relevant OMB memoranda include, but are not limited to, the following:

- OMB M-07-18.
- Annual FISMA reporting instructions (e.g. OMB M-07-19, OMB M-08-21).

f. NIST SP 800-23 must be used as guidance on the acquisition and use of tested/evaluated IT products.

g. NIST SP 800-35 must be used as guidance when deciding on IT security services.

h. NIST SP 800-36 must be used as guidance when selecting information security products.

i. NIST SP 800-64, Revision 2 must be used as guidance regarding security considerations in the SDLC.

j. NIST SP 800-70, Revision 2 must be used as guidance on configuration settings for IT products.

For moderate and high information systems

k. Vendors and contractors must provide information in acquisition documents that describes the functional properties of the security controls to be employed within the information system, information system components, or information system services, with sufficient detail to permit independent analysis and testing of the controls.

l. Each information system component acquired must be explicitly assigned to an information system and the owner of the system must acknowledge this assignment.

For high information systems

m. Vendors and contractors must provide information in acquisition documents that describes the design and implementation details of the security controls to be employed within the information system, information system components, or information system services (including functional interfaces among control components), with sufficient detail to permit independent analysis and testing of the controls.

SA- 5 – Information System Documentation

a. Administrator documentation (i.e., whether published by a vendor/manufacturer or written in-house) for the information system and constituent components must be obtained, protected as required, and made available to authorized personnel.
    i. Administrator documentation must include information that describes:
        - Secure configuration, installation, and operation of the information system.
        - Effective use and maintenance of the system's security features/functions.
        - Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions.

b. User documentation (i.e., whether published by a vendor/manufacturer or written in-house) for the information system and constituent components must be obtained, protected as required, and made available to authorized personnel.
    i. User documentation must include information that describes:
        - User-accessible security features/functions and how to effectively use those security features/functions.
        - Methods for user interaction with the information system, which enables individuals to use the system in a more secure manner.
        - User responsibilities in maintaining the security of the information and information system.

c. Security documentation must be updated throughout the information system's life cycle.

d. When information system documentation is either unavailable or non- existent, the following actions must be taken:
    i. Document attempts to obtain such documentation.

ii. Recreate selected information system documentation if such documentation is essential to the effective implementation and/or operation of security controls.

For moderate and high information systems

e. Vendor/manufacturer documentation describing the functional properties of the security controls employed within the information system, with sufficient detail to permit independent analysis and testing, must be obtained, protected as required, and made available to authorized personnel.

f. Vendor/manufacturer documentation describing the high-level design of the information system in terms of subsystems and implementation details of the security controls employed within the system, with sufficient detail to permit independent analysis and testing, must be obtained, protected as required, and made available to authorized personnel.

For high information systems

g. Vendor/manufacturer documentation describing the security-relevant external interfaces to the information system, with sufficient detail to permit independent analysis and testing, must be obtained, protected as required, and made available to authorized personnel.

SA- 6 – Software Usage Restrictions

a. Software usage restrictions must be complied with.
    i. The System Owner (SO) shall ensure the rules of behavior for the information system states that users must abide by software copyright laws and shall not obtain, install, replicate, or use unlicensed software.
        - Refer to *Information Security – Interim Security Planning Procedures* for requirements on rules of behavior.

b. Software and associated documentation must be used in accordance with contract agreements and copyright laws.

c. For software and associated documentation protected by quantity licenses, tracking systems must be employed to control copying and distribution.

Note: Tracking systems can include, for example, simple spreadsheets or fully automated, specialized applications depending on the needs of the organization.

d. The use of peer-to-peer file sharing technology is prohibited.

e. The use of instant messaging to communicate with anyone outside of EPA is strictly prohibited except through EPA approved standards.

Note: Instant messaging tools include, but are not limited to, Qnext, Windows Live Messenger, AOL Instant Messenger (AIM), Yahoo! Messenger, Skype, Google Talk, .Net Messenger Service, Jabber, Internet Relay Chat (IRC), QQ, Excite PAL iChat, and ICQ).

f. Only licensed and registered software may be installed and used on EPA information systems.
    i. Freeware or shareware must not be used unless properly authorized by an appropriate EPA official.

g. Installation of any non-standard software, including shareware and freeware, must be controlled and documented by the SO to ensure the following:
    i. The SO and office or regional management shall accept all risks, accountability, and responsibility for issues and incidents associated with installation of any non-standard software. This acceptance includes, but is not limited to:
        - Vulnerabilities that have not been identified.
        - Actions that have not been complied with pursuant to these procedures.
    ii. Risks to the EPA network or other interconnected systems must have been identified, communicated to, and approved by the SOs of those systems, prior to installation of the non-standard software.
        - Refer to *Information Security – Interim Security Assessment and Authorization Procedures* for requirements on information system interconnections.
    iii. There must be a bona fide business need for the non-standard software and the functionality or capability is not available with any Agency-standard software.
    iv. Mandatory federal standards and requirements must not be subverted or avoided.
    v. Installation of the software must not violate any license agreements or contract requirements.
    vi. The software capability must not be used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.
    vii. The software must not have multi-user recast / peer-to-peer functionality (e.g., Skype, Napster).
    viii. The vendor site and NIST's National Vulnerability Database (NVD) must have been researched prior to installation to identify and address:
        - All known vulnerabilities.
        - Mitigation of all vulnerabilities.
    ix. Procedures must be in place to:
        - Track any future security vulnerabilities.
        - Request installation of necessary security fixes or patches as they arise.
    x. Tests of the software must be conducted off-network.
    xi. Tests must prove that the installed software does not:
        - Alter Agency USGCB configuration settings or require permanent alteration or waivers of configuration settings.

- Install malicious software, adware or spyware.
- Communicate without the user's knowledge or authorization any information, whether that information is confidentially sensitive or not.

xii. The EPA Call Center and information system support must be contacted immediately when any security issues with the software are identified.

xiii. The software must be uninstalled when any security issues are identified, unless patches can be installed within a timeframe consistent with the risks presented.

xiv. Annual security awareness and training must address use of the non-standard software.

SA- 7– User-Installed Software

a. Users are prohibited from installing any software on EPA's information systems that does not meet one of the following conditions:
   i. The software must conform to Agency-approved standards, including configuration standards.
   ii. The installation of non-Agency standard software (including public domain software such as freeware or shareware) must be authorized in writing by the SO and the Information Security Officer (ISO).

b. The SO shall ensure the rules of behavior for the information system specify that only authorized software may be installed on EPA's equipment and networks.
   i. Refer to *Information Security – Interim Security Planning Procedures* for requirements on rules of behavior.

c. Approved and permitted software, whether Agency-standard or non-standard, must be installed on EPA equipment in accordance with the requirements found under *SA-6 – Software Usage Restrictions* of this document.

d. EPA shall identify the types of software installations that are permitted. Categories of permitted software installations include:
   i. Approved and tested updates and security patches to existing software.
   ii. EPA developed software.

e. EPA shall identify the types of software downloads that are prohibited. Categories of prohibited software downloads include:
   i. Unauthorized install-on-demand software.
   ii. Software whose pedigree with regard to being potentially malicious is unknown or suspect.
   iii. Untested unauthorized software.
      - Refer to *SA-6 – Software Usage Restrictions*.

f. Rules governing the downloading and installation of software by users must be strictly enforced by information system personnel.
   i. Administrative rights must be removed for any violations of policies and procedures and not restored until appropriate counseling and remediation has taken place.

ii. Administrative rights may be denied in the future.

g. The information system must be tested for prohibited software by using a scanner which detects and reports the names of installed software and the results must be compared against the approved software applications list.
    i. Refer to *Information Security – Interim Risk Assessment Procedures* for requirements on scanners.

SA- 8– Security Engineering Principles

For moderate and high information systems

a. Information system security engineering principles must be applied in the specification, design, development, implementation, and modification of the information system.
b. The application of security engineering principles must be integrated into the SDLC.
    i. Security engineering principles are primarily targeted at information systems under new development and information systems undergoing major upgrades.
    ii. For legacy information systems, security engineering principles must be applied to system upgrades and modifications, to the extent feasible, given the current states of the hardware, software, and firmware components within the system.
c. Security engineering principles must include, but are not limited to:
    i. Developing layered protections.
    ii. Establishing sound security policy, architecture, and controls as the foundation for design.
    iii. Incorporating security into the SDLC.
    iv. Delineating physical and logical security boundaries.
    v. Ensuring system developers and integrators are trained on how to develop secure software.
    vi. Tailoring security controls to meet organizational and operational needs.
    vii. Reducing risk to acceptable levels, thus enabling informed risk management decisions.
d. NIST SP 800-27, Revision A must be used as guidance on engineering principles for information system security.

SA- 9– External Information System Services

a. Documents that solicit and implement external information system services must require that providers comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.
b. Documents that solicit and implement external information system services must:
    i. Identify specific drivers for soliciting the services.
        - Examples include, but are not limited to applicable federal laws,

Executive Orders, directives, policies, regulations, standards, and guidance.

ii. Specify responsibilities for each security control or for specific activities within a control.

iii. Identify associated reporting requirements for each security control.

iv. Require the provider of external information system services to conform to the same security control and documentation requirements as would apply to the Agency's internal systems.

- However, it is not necessary for the provider to employ EPA-specific templates for documentation.

c. The following documentation must be included in the procurement of external information system services:

i. Government, service provider, and end user security roles and responsibilities.

ii. Any SLAs.

d. SLAs must:

i. Define expectations of performance for each required security control.

ii. Describe measurable outcomes.

iii. Specify remedies and response requirements for any identified instance of non-compliance.

e. A chain of trust or level of confidence must be established with external service providers to ensure adequate protection of services rendered.

i. Risks must be assessed in the risk assessment process.

ii. Risks must be documented.

iii. The extent and nature of the chain of trust varies based on the relationship between EPA and the external provider.

iv. Where a sufficient level of trust cannot be established in the external services and/or service providers, the following must be adhered to:

- Employ compensating security controls or accept the greater degree of risk.
- Confer with the Senior Agency Information Security Officer (SAISO) and the Chief Technology Officer (CTO) regarding risks associated with the network and Agency.

f. Risks that arise from the use of external information system services must be adequately mitigated.

g. Security control compliance by the external information system service providers must be monitored.

h. NIST SP 800-35 must be used when deciding on IT security services.

i. NIST SP 800-64, Revision 2 must be used regarding security considerations in the SDLC.

SA- 10– Developer Configuration Management

For moderate and high information systems

a. Configuration management must be performed during information system design, development, implementation, and operation for:
    i. Contractual development and system integration.
    ii. Internal development procedures.
b. The configuration management process must address the following:
    i. Managing and controlling changes to the information system.
    ii. Implementing only EPA-approved changes.
    iii. Documenting approved changes to the information system.
    iv. Tracking of security flaws and corrective or remediation actions.

SA- 11– Developer Security Testing

For moderate and high information systems

a. Testing requirements must be included in:
    i. Contractual documents for development and system integration.
    ii. Internal development procedures.
b. A Security Test and Evaluation Plan must be created and implemented for all information system development.
    i. The plan must be developed in consultation with associated security personnel, including security engineers.
    ii. Using automated code analysis tools is a preferred testing methodology, has proved to be an efficient testing mechanism, and provides better assurance than manual code walk-throughs.
    iii. Vulnerability scanning must be a component of the testing
        - The information system and its configuration must be scanned prior to authorization and again immediately following deployment.
    iv. When NIST-validated cryptographic modules are used, the following must be verified:
        - The existence of a valid certificate for each module.
        - Conformance to the published security policy for each module employed.
    v. The plan must include requirements for retesting after significant changes occur.
c. A verifiable flaw remediation process must be implemented to correct weaknesses and deficiencies identified during the security testing and evaluation process.
d. Results of the security testing/evaluation and flaw remediation processes must be documented.
e. Developmental security test results, after verification, must be used to the greatest extent feasible.

Note: It must be recognized that these results are impacted (i.e., they may no longer be valid) whenever there have been security-relevant modifications to the information system subsequent to developer testing. In addition, new threats can render security test results less relevant or irrelevant.

i. Use of these test results must include providing evidence for and documenting one of the following:
   - A control is in place and operating as intended (for a positive test result).
   - A control is either not in place or not operating as intended (for negative test results).

f. Those controls not in place or not operating as intended, as determined by test results, must be remediated.
   i. The plan for remediation must be entered into and tracked in the EPA POA&M repository.
   ii. The EPA POA&M repository must be used.
      - For all systems that are reportable to OMB.
      - For non-reportable systems, when feasible.

Note: Using the EPA POA&M repository for a non-reportable system will assist in a smooth and accurate transition for yet uncompleted control remediations whose risks have been accepted by the Authorizing Official (AO) when the information system becomes OMB reportable.

g. Developmental security test results must be used in support of the security authorization process for the delivered information system.
   i. Use of these results must be dependent on the following:
      - How current or recent the test results are.
      - The judgment of the independent authorization agent as to their applicability.

SA- 12– Supply Chain Protection

For high information systems

a. Measures to protect against supply chain threats (Draft NISTIR-7622) must be employed as part of a comprehensive, defense-in-breadth information security strategy to protect against supply chain threats.
   i. Vulnerabilities must be identified, managed, and eliminated at each phase of the life cycle.
   ii. Risk must be mitigated by the use of complementary, mutually reinforcing strategies.

Note: A defense-in-breadth approach helps to protect information systems (including the information technology products that compose those systems) throughout the system development life cycle (i.e., during design and development, manufacturing, packaging, assembly, distribution, system integration, operations, maintenance, and retirement).

SA- 13– Trustworthiness

For high information systems

Note: The intent of this control is to ensure that organizations recognize the importance of trustworthiness and making explicit trustworthiness decisions when designing, developing, and implementing organizational information systems.

a. The information system must meet appropriate levels of trustworthiness.
    i. If risk resultant from highly-skilled threat agent (e.g., state sponsored) is unacceptable by AO or CIO, the system shall meet a high level of trustworthiness.
    ii. Where high is defined as having those affected controls, determined in the risk assessment, provide sufficient functionality and are tested to ensure the functionality is effective to reduce the elevated risks to an acceptable level.

Note: Two factors affecting the trustworthiness of an information system include: (i) security functionality (i.e., the security features or functions employed within the system); and (ii) security assurance (i.e., the grounds for confidence that the security functionality is effective in its application).

b. Appropriate security functionality for the information system must be obtained by using Steps 1, 2, and 3 of the Risk Management Framework (RMF) to select and implement the necessary management, operational and technical security controls necessary to mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation.
c. Appropriate security assurance must be obtained by:
    i. The actions taken by developers and implementers of security controls with regard to the design, development, implementation, and operation of those controls.
    ii. The actions taken by assessors to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system.

Note: Developers and implementers can increase the assurance in security controls by employing well-defined security policy models, structured, disciplined, and rigorous

hardware and software development techniques, and sound system/security engineering principles. Assurance is also based on the assessment of evidence produced during the initiation, acquisition/development, implementation, and operations/maintenance phases of the system development life cycle. For example, developmental evidence may include the techniques and methods used to design and develop security functionality. Operational evidence may include flaw reporting and remediation, the results of security incident reporting, and the results of the ongoing monitoring of security controls. Independent assessments by qualified assessors may include analyses of the evidence as well as testing, inspections, and audits. Minimum assurance requirements are described in Appendix E of NIST SP 800-53, Revision 3.

Note: Explicit trustworthiness decisions highlight situations where achieving the information system resilience and security capability necessary to withstand cyber-attacks from adversaries with certain threat capabilities may require adjusting the risk management strategy, the design of mission/business processes with regard to automation, the selection and implementation rigor of management and operational protections, or the selection of information technology components with higher levels of trustworthiness. Trustworthiness may be defined on a component-by-component, subsystem-by-subsystem, or function-by-function basis. It is noted, however, that typically functions, subsystems, and components are highly interrelated, making separation by trustworthiness perhaps problematic and at a minimum, something that likely requires careful attention in order to achieve practically useful results.

d. NIST SP 800-23 must be used as guidance on the acquisition and use of tested/evaluated IT products.
e. NIST SP 800-53, Revision 3 must be used as guidance on the selection and implementation of security controls in information systems.
f. NIST SP 800-53A, Revision 1 must be used as guidance for the assessment of security controls.
g. NIST SP 800-60, Revision 1 must be used as guidance for mapping information systems to security categories.
h. NIST SP 800-64, Revision 2 must be used as guidance regarding security considerations in the SDLC.

7. RELATED DOCUMENTS

- NIST SP 800-23, *Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products*, August 2000
- NIST SP 800-27, Revision A, *Engineering Principles for Information Technology Security*, June 2004
- NIST SP-35, *Guide to Information Technology Security Services*, October 2003
- NIST SP-36, *Guide to Selecting Information Technology Security Products*, October 2003
- NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009

- NIST SP 800-53A, Revision 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*, June 2010
- NIST SP 800-60, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008
- NIST SP 800-64, Revision 2, *Security Considerations in the System Development Life Cycle,* October 2008
- NIST SP 800-65, *Integrating IT Security into the Capital Planning and Investment Control Process,* January 2005
- NIST SP 800-70, Revision 2, *National Checklist Program for IT Products: Guidelines for Checklist Users and Developer*, February 2011

8. ROLES AND RESPONSIBILITIES

Office of Technology Operations and Planning (OTOP), Environmental Information (OEI)

a. OTOP has the following responsibilities with respect to system and services acquisition:
   i. Perform an analysis on each investment submitted by the Program Offices to ensure life cycle requirements are being met.

Office of Administration and Resources Management (OARM)

b. OARM has the following responsibilities with respect to system and services acquisition:
   i. Ensure that acquisition documents and agreements contain appropriate language for information systems, services, and IT resource acquisitions.

Senior Agency Information Security Officer (SAISO)

c. The SAISO has the following responsibilities with respect to system and services acquisition:
   i. Provide oversight of the Agency's system and services activities.
   ii. Work with OARM to ensure that appropriate standard language is developed for acquisition documents and agreements for information systems, services, and IT resource acquisitions.
   iii. Review submission proposals for IT investments for consistency and conformance to security requirements of the life cycle.

Senior Information Official (SIO)

d. The SIO has the following responsibilities with respect to system and services acquisition:
   i. Ensure that security is integrated into the life cycle process for their information systems.
   ii. Ensure acquisition of information systems, services and IT resources complies with security requirements.
   iii. Ensure submission proposals for IT investments to the Agency's CIO

conform to security requirements of the life cycle.

iv. Establish Office- or Regional-specific policies and procedures as needed to supplement Agency and federal policies and procedures.

v. Ensure allocation of resources to protect the information system in acquisition planning and investments.

vi. Understand risks associated with external information systems and services.

vii. Ensure that risks that arise from the use of external information system services are adequately mitigated.

viii. Require that an appropriate chain of trust be established with external service providers when dealing with the many issues associated with information security.

ix. Develop a defense-in-breadth information security strategy to protect against supply chain threats.

Authorizing Official (AO)

e. The AO has the following responsibilities with respect to system and services acquisition:

i. Ensure that risks that arise from the use of external information system services are adequately mitigated.

ii. Require that an appropriate chain of trust be established with external service providers when dealing with the many issues associated with information security.

Information Security Officer (ISO)

f. The ISO has the following responsibilities with respect to system and services acquisition:

i. Assist the SO and SIO in carrying out their responsibilities.

ii. Ensure that management and relevant information system personnel are aware of their responsibilities for system and services acquisition.

iii. Ensure acquisition of information systems, services and IT resources complies with security requirements.

iv. Ensure submission proposals for IT investments to the Agency's CIO conform to security requirements of the life cycle.

v. Review acquisition documents for compliance and completeness.

vi. Ensure security control compliance monitoring of external service providers and assist in improving efficiency and effectiveness of monitoring across the organization.

vii. Recommend enterprise efficiencies as needed.

System Owner (SO)

g. The SO has the following responsibilities with respect to system and services acquisition:

i. Identify the security requirements for the information system throughout the SDLC.
ii. Coordinate security and functional requirements throughout the entire SDLC.
iii. Ensure the rules of behavior for the information system states that users must abide by software copyright laws and shall not obtain, install, replicate, or use unlicensed software.
iv. Ensure the rules of behavior for the information system specifies that only authorized software shall be installed on EPA's equipment and networks.
v. Grant or deny approval to users to install non-EPA or public domain software (e.g., freeware, shareware) on their workstations.
vi. Monitor compliance with software usage restrictions on the information system.
vii. Submit proposals for IT investments to the Program or Regional office management approval chain that conform to security requirements of the life cycle.
viii. Ensure information system documentation is developed and delivered.
ix. Implement information system security engineering principles in the acquisition and development of information systems.
x. Ensure security control compliance of external service providers is monitored.
xi. Ensure acquisition documents address security requirements and contain appropriate language.
xii. Acknowledge the assignment of information system components acquired explicitly for the information system.
xiii. Obtain appropriate security functionality for the information system by using the RMF to select and implement security controls.
xiv. Assist the SIO in carrying out their responsibilities for system and services acquisition.
xv. Ensure acquisition of information systems, services and IT resources complies with security requirements.
xvi. Approve acquisition of non-standard software.
xvii. Ensure submission proposals for IT investments to the Agency's CIO conform to security requirements of the life cycle.
xviii. Recommend to the SIO efficient methods for monitoring across the organization security controls that are the responsibility of external service providers and appropriate allocation of resources.
xix. Oversee proper, efficient, and effective implementation of security engineering principles within the program or Regional office's acquisition and development activities.

Information System Security Officer (ISSO)

h. The ISSO has the following responsibilities with respect to system and services

acquisition:

i. Assist the SO in complying with security requirements throughout the entire SDLC and lead the security requirements efforts.
ii. Analyze, test, and approve, if appropriate, non-standard software in accordance with procedures.
iii. Review acquisition documents of the information system for compliance and completeness.
iv. Review documentation for completeness and compliance.
v. Monitor security control compliance of external service providers.

Information System Developers

i. Information system developers have the following responsibilities with respect to system and services acquisition:
    i. Develop and maintain adequate information system documentation in accordance with requirements.
    ii. Integrate security engineering principles into SDLC methodologies.
    iii. Ensure the information system is protected from threats and establish chains of trust within the life cycle activities.
    iv. Ensure independence of security testing, verification, and validation within the system's life cycle.
    v. Ensure federal and Agency architectures and standards are the first consideration in development of information systems.
    vi. Create a Security Test and Evaluation Plan, implement the plan, document the results, and implement a flaw remediation process.
    vii. Take actions to increase the security assurance in the security controls of the information system.

9. DEFINITIONS

- Chain of Trust – occurs when each component of hardware and software for an information system is validated. The purpose is to ensure that only trusted components are used.
- External Information System Service - a service that is implemented outside of the authorization boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system). Relationships with external service providers are established in a variety of ways, for example, through joint ventures, business partnerships, outsourcing arrangements (i.e., contracts, interagency agreements, lines of business arrangements), licensing agreements, and/or supply chain exchanges.
- Information System - a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
- Signature (of an individual) – a mark or sign made by an individual to signify knowledge, approval, acceptance, or obligation. Can be accomplished manually,

sometimes referred to as a "wet signature," or electronically.

- Trustworthiness – a characteristic or property of an information system that expresses the degree to which the system can be expected to preserve the confidentiality, integrity, and availability of the information being processed, stored, or transmitted by the system.
- Trustworthy Information Systems – systems that are capable of being trusted to operate within defined levels of *risk* despite the environmental disruptions, human errors, and purposeful attacks that are expected to occur in the specified environments of operation.
- Written – or "in writing" means to officially document the action or decision and includes a signature. The documentation can be accomplished manually or electronically.

10. WAIVERS

Waivers may be requested from the CIO by submitting a justification based on:

- substantive business case need(s)
- demonstration of, or a proposal for, establishment of adequate compensating controls that provide a suitable alternative to the mandated protection

The CIO may grant a waiver for sufficient reasons exercising judgment in the best interests of the Agency.

The SAISO and Director, OTOP shall coordinate to maintain central repository of all waivers.

11. RELATED POLICY, PROCEDURES, STANDARDS AND GUIDELINES

Related policy and procedures are available on OEI's Policy Resources website.
http://intranet.epa.gov/oei/imitpolicy/policies.htm
Related standards and guidelines are available on OEI's website.

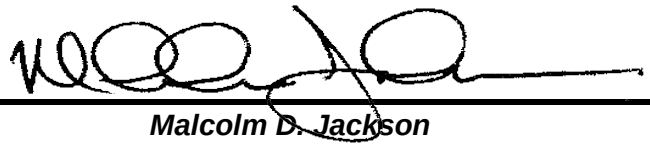
12. MATERIAL SUPERSEDED

NA

13. ADDITIONAL INFORMATION

- Software Assurance, US-CERT (Computer Emergency Readiness Team) - http://www.us-cert.gov/swa/
- Build Security In, US-CERT - https://buildsecurityin.us-cert.gov/daisy/bsi/home.html

EPA Classification No.:	CIO-2150.3-P-15.1	CIO Approval Date:	08/06/2012
CIO Transmittal No.:	12-003	Review Date:	08/06/2015



Malcolm D. Jackson
Assistant Administrator and Chief Information Officer
Office of Environmental Information

APPENDIX A: ACRONYMS

AIM	AOL Instant Messenger
AO	Authorizing Official
BIA	Business Impact Assessment
CIO	Chief Information Officer
CPIC	Capital Planning and Investment Control
CTO	Chief Technology Officer
EPA	Environmental Protection Agency
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
IRC	Internet Relay Chat
ISO	Information Security Officer
ISSO	Information System Security Officer
IT	Information Technology
MOU/A	Memorandum of Understanding/Agreement
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
O&M	Operations and Maintenance
OARM	Office of Administration and Resources Management
OEI	Office of Environmental Information
OMB	Office of Management and Budget
OTOP	Office of Technology Operations and Planning
PIA	Privacy Impact Assessment
POA&M	Plan of Action and Milestones
RMF	Risk Management Framework
SAISO	Senior Agency Information Security Officer
SDLC	System Development Life Cycle
SIO	Senior Information Official
SLA	Service Level Agreement
SO	System Owner
SP	Special Publication
SSP	System Security Plan
USA PATRIOT	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism
USC	United States Code
US-CERT	United States Computer Emergency Readiness Team
USGCB	United States Government Configuration Baseline

DOCUMENT CHANGE HISTORY

Version	Release Date	Summary of Changes	Author of Changes	DCN
0.6	2/6/2008	Initial draft	Heather Flager	Procedures-SA-Draft_TO62_020_1
2.0	6/29/2009	Incorporated EPA comments Final	Heather Flager	Procedures-SA-Final_TO62_020_2
2.8	8/5/2010	Updated per NIST SP 800-53 Rev 3	Heather Flager	Procedures_SA_Draft.TO-062_050_1
2.8	8/19/2010	TISS Initial reviews and comments	Charleen Johnson	Procedures_SA_Draft.TO-062_050_1
2.9	12/27/2010	TISS Final Draft Review	Charleen Johnson	Procedures_SA_Draft.TO-062_050_1
3.0	5/1/2012	SAISO Final Review	David Stepp	Procedures_SA_Draft.TO-062_050_1
3.1	7/17/2012	Document Review	LaToya Gordon	Procedures_SA_Draft.TO-062_050_1